



PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS



TIPICO GROUP LTD.

Tipico Tower
Vjal Portomaso
St. Julian's, STJ 4011, Malta

[www.tipico-
group.com](http://www.tipico-group.com)

Version 2.0 - October 2026

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	2

CONTENTS

1.	ABOUT THIS PRIVACY STATEMENT.....	4
2.	WHO IS RESPONSIBLE FOR YOUR PERSONAL DATA?	4
3.	WHO DOES THIS PRIVACY STATEMENT APPLY TO?	5
4.	WHAT PERSONAL DATA DO WE PROCESS AND WHERE DO WE OBTAIN IT?	5
5.	WHY DO WE PROCESS YOUR PERSONAL DATA?	8
6.	DUE DILIGENCE AND BUSINESS-PARTNER SCREENING.....	9
7.	VISITORS, CONTRACTORS AND PHYSICAL SECURITY.....	10
8.	WITH WHOM DO WE SHARE PERSONAL DATA?	11
9.	INTERNATIONAL TRANSFERS	11
10.	HOW LONG DO WE RETAIN PERSONAL DATA?	12
11.	IS PROVIDING PERSONAL DATA MANDATORY?	13
12.	AUTOMATED DECISION-MAKING AND PROFILING.....	13
13.	DATA SECURITY.....	14
14.	YOUR DATA-PROTECTION RIGHTS.....	14
15.	COMPLAINTS AND SUPERVISORY AUTHORITIES.....	15
16.	CONTACTING THE DATA PROTECTION OFFICER.....	15
17.	CHANGES TO THIS PRIVACY STATEMENT	16
18.	DOCUMENT CONTROL	16

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	3

1. ABOUT THIS PRIVACY STATEMENT

Tipico is committed to protecting personal data and processing it fairly, lawfully and transparently.

This Privacy Statement explains how the relevant company within the Tipico Group processes personal data relating to:

- suppliers, service providers and contractors;
- representatives, directors, shareholders, beneficial owners, employees and subcontractors of suppliers and business partners;
- potential and existing business partners;
- consultants, professional advisers and other external contacts;
- visitors, guests, couriers, delivery personnel and other persons entering Tipico premises; and
- other individuals whose personal data is processed in connection with Tipico's business relationships, procurement activities, due-diligence processes, visitor management or physical-security operations.

This Privacy Statement does not apply to the processing of personal data relating to Tipico customers, job applicants or employees where a separate privacy statement applies.

"Personal data" means any information relating to an identified or identifiable natural person. Information relating only to a legal entity is not personal data, although information relating to individual representatives, employees, shareholders or beneficial owners of that entity may constitute personal data.

This Privacy Statement provides information under Articles 13 and 14 of the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR") and can be found on our [group website](#).

This Privacy Statement may be subject to modification from time to time, notably in the event of changes to legislation, the introduction of new laws or revision or expansion of our offering. Any changes will be published on our website. We therefore recommend that you check the Privacy Statement regularly.

2. WHO IS RESPONSIBLE FOR YOUR PERSONAL DATA?

The data controller is the Tipico Group company that determines why and how your personal data is processed, as further explained below.

Where more than one Tipico Group company (Tipico Group Ltd. and all its subsidiaries, (hereinafter "Tipico", "we", "us", "our")) jointly determines the purposes and means of a processing activity, those companies may act as joint controllers. Information about the essence of the relevant arrangement may be obtained from the Group Data Protection Officer.

For supplier and business-partner processing, the controller will normally be the Tipico Group company that:

- is named in the relevant contract, purchase order, tender documentation or business

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	4

- correspondence;
- is considering entering into or has entered into the relevant business relationship; or
- conducts the relevant due-diligence or compliance process.

For visitor and physical-security processing, the controller will normally be the Tipico Group company operating or responsible for the premises you visit. The identity and contact details of the relevant controller are stated in the visitor notice displayed at the relevant premises or made available during visitor registration.

The contact details of the relevant controller are stated in the applicable contract, purchase order, invitation, correspondence or location-specific visitor notice. You may also contact the Group Data Protection Officer at dpo@tipico.com if you require confirmation of the identity of the controller responsible for a particular processing activity.

3. WHO DOES THIS PRIVACY STATEMENT APPLY TO?

This Privacy Statement applies where Tipico processes personal data relating to:

- individual suppliers, contractors or consultants;
- directors, officers, employees, representatives and contact persons of suppliers and business partners;
- shareholders, beneficial owners and authorised signatories;
- subcontractors and their representatives or employees;
- potential suppliers and participants in procurement or tender processes;
- advisers, auditors and other professional contacts;
- visitors, guests, contractors, couriers and delivery personnel;
- persons named in visitor, delivery, key, access, patrol, handover or security-incident records; and
- other individuals involved in a current or prospective business relationship with Tipico.

If you provide personal data relating to another individual, you should ensure that you are authorised to provide that information and, where appropriate, make this Privacy Statement available to that individual.

4. WHAT PERSONAL DATA DO WE PROCESS AND WHERE DO WE OBTAIN IT?

Identification and contact information

- name, title and business contact details;
- organisation, employer, position and professional responsibilities;
- signature and authorised-signatory information;
- identification documents or identification numbers where required for a lawful and documented purpose.

Business-relationship information

- contractual and commercial correspondence;
- information contained in contracts, purchase orders and tender documentation;
- services provided, project responsibilities and relationship history;
- meeting information, business communications and records of decisions;
- complaints, queries and dispute-related information.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	5

Financial and payment information

- bank-account and payment information;
- invoices, transaction details and tax-related information;
- information necessary for accounting, audit and payment administration.

Due-diligence and compliance information

- corporate ownership and management information;
- information concerning shareholders, beneficial owners, directors and authorised representatives;
- sanctions, politically exposed person and adverse-media screening results;
- conflicts-of-interest information;
- information necessary for regulatory, licensing, anti-fraud, anti-bribery, anti-money laundering or other compliance checks;
- information concerning criminal convictions or alleged offences only where processing is authorised by applicable law.

Technical and security information

- system account and access information;
- IP address, device, authentication and system-usage information;
- information-security events, access logs and audit records;
- information required to protect Tipico systems, networks, premises and assets.

Visitor and physical-security information

- name and organisation;
- host or Tipico contact person;
- purpose, date and time of the visit;
- arrival and departure time;
- signature, where required;
- visitor badge and access details;
- delivery and parcel collection information;
- key issuance and return information;
- vehicle registration details where required for parking or site access;
- information recorded in visitor, access, patrol, handover, occurrence or security-incident logs;
- CCTV footage where cameras are in operation.

Sources of personal data

We may obtain personal data:

- directly from you;
- from your employer, organisation or another business partner;
- from Tipico employees involved in the relationship;
- from publicly available registers, websites and professional sources;
- from public authorities and regulatory bodies;
- from compliance, fraud-prevention, sanctions-screening, credit-reference and due-diligence providers;

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	6



- from Tipico access-control, visitor-management, security and IT systems; and
- from contracted reception or security-service providers.

Where personal data has not been obtained directly from you, Tipico provides the information required under Article 14 GDPR within the applicable period and subject to any lawful exception.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	7

5. WHY DO WE PROCESS YOUR PERSONAL DATA?

Please find below for each processing activity and purpose the categories of data typically involved and the legal basis

Processing activity and purpose	Categories typically involved	Legal basis
Managing requests for information, tenders, negotiations and supplier onboarding	Identification, contact, professional and business-relationship information	Article 6(1)(b) GDPR where the individual is a party to the prospective contract; otherwise Article 6(1)(f), Tipico's legitimate interest in identifying and engaging suitable business partners
Entering into, administering and performing contracts	Identification, contact, contractual, project and service information	Article 6(1)(b) where the individual is a contractual party; otherwise Article 6(1)(f), Tipico's legitimate interest in managing contractual relationships
Procurement, supplier and relationship management	Identification, business-contact, service and correspondence information	Article 6(1)(f), Tipico's legitimate interests in effective procurement, supplier management and business administration
Invoice, payment, accounting, tax and audit administration	Identification, financial, transactional and contractual information	Article 6(1)(b), where applicable; Article 6(1)(c), compliance with accounting, tax and audit obligations; Article 6(1)(f), financial administration and fraud prevention
Supplier and business-partner due diligence	Identification, ownership, management, compliance and risk information	Article 6(1)(c), where checks are legally required; Article 6(1)(f), Tipico's legitimate interests in regulatory compliance, partner-risk management, fraud prevention and protecting its business
Sanctions, politically exposed person, anti-bribery, conflict-of-interest and adverse-media screening	Identification, role, ownership and compliance information	Article 6(1)(c), where required by law; Article 6(1)(f), Tipico's legitimate interests in preventing financial crime, corruption, fraud and reputational harm
Information-security, account and access management	Identification, system-account, device, authentication and access-log information	Article 6(1)(c), where required by law or regulation; Article 6(1)(f), Tipico's legitimate interests in protecting systems, information, personnel and business operations
Compliance monitoring, investigations and whistleblowing	Identification, correspondence, allegations, investigation and evidence information	Article 6(1)(c), where processing is legally required; Article 6(1)(f), Tipico's legitimate interests in identifying and investigating misconduct and protecting legal rights
Establishing, exercising or defending legal claims	Contractual, correspondence, transaction, security and dispute information	Article 6(1)(f), Tipico's legitimate interest in protecting and enforcing its legal rights
Business communications and relationship development	Business-contact, role, preference and communication information	Article 6(1)(f), Tipico's legitimate interests in maintaining professional relationships; consent where required by applicable electronic-communications law
Visitor registration and premises access	Identification, organisation, host, purpose, arrival, departure, badge and access information	Article 6(1)(f), Tipico's legitimate interests in managing access and maintaining secure premises
Deliveries, parcel collection and key management	Identification, signature, delivery, collection, key and timestamp information	Article 6(1)(f), Tipico's legitimate interests in maintaining custody, accountability and physical security
Security patrols, guard handovers, occurrence records and incident management	Identification, access, security-event, observation and incident information	Article 6(1)(f), Tipico's legitimate interests in protecting persons, premises, operations and assets; Article 6(1)(c) where legal health-and-safety or security obligations apply
Anti-money laundering, counter-terrorist financing and financial-crime risk assessment, monitoring, investigation and regulatory reporting	Identification, ownership, financial, source-of-funds, source-of-wealth, screening, risk-assessment, investigation and compliance information	Article 6(1)(c) GDPR where processing is required by applicable law or regulation; otherwise Article 6(1)(f) GDPR, Tipico's legitimate interests in preventing, detecting and managing financial-crime risk and protecting its business, assets and reputation
CCTV operation	Images and associated date, time and location information	Article 6(1)(f), Tipico's legitimate interests in preventing, detecting and documenting security and safety incidents; further information is provided in the applicable CCTV notice

Where special-category personal data is processed, Tipico will identify both an Article 6 legal basis and an applicable condition under Article 9 GDPR. Where data relating to criminal convictions or offences is processed, Tipico will do so only under the control of official authority or where authorised by applicable Union or Member State law in accordance with Article 10 GDPR.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	8

Tipico does not rely on consent where another legal basis is more appropriate. Where consent is used, it is voluntary and may be withdrawn at any time without affecting processing carried out before withdrawal.

6. DUE DILIGENCE AND BUSINESS-PARTNER SCREENING

Tipico may carry out proportionate due-diligence checks before and during a business relationship. The nature and extent of the checks depend on factors including the services concerned, value and duration of the relationship, geographic exposure, access to Tipico information or systems, regulatory requirements and the risks associated with the relationship.

Due-diligence activities may include:

- verifying identity, company registration and authority to represent an organisation;
- identifying directors, shareholders and beneficial owners;
- sanctions and politically exposed person screening;
- anti-bribery, anti-corruption, anti-fraud, anti-money laundering and conflict-of-interest checks;
- financial, credit and business-continuity checks;
- assessing information-security and data-protection controls;
- adverse-media and reputational-risk screening;
- ESG related assessments (may include information concerning environmental, labour, human-rights, ethical-business-conduct or sustainability practices where relevant to the services provided or the supplier's risk profile)
- verifying licences, qualifications or regulatory status; and
- ongoing monitoring where justified by law or the assessed risk.

Information may be obtained from you, your organisation, publicly available sources, official registers, public authorities and specialist due-diligence or screening service providers.

The legal basis is Article 6(1)(c) GDPR where the check is required by law, and otherwise Article 6(1)(f) GDPR. Tipico's legitimate interests include regulatory compliance, preventing fraud and financial crime, assessing prospective and existing business partners, protecting Tipico's assets and reputation and ensuring that business relationships meet Tipico's legal, security and ethical requirements.

Due diligence and compliance reviews may be repeated periodically or triggered by significant changes to the supplier, the services provided, ownership structure, geographic exposure, regulatory requirements or assessed risk level.

Where required by applicable anti-money laundering, counter-terrorist financing, licensing or other financial-crime legislation, or where justified by Tipico's legitimate interests in preventing and managing financial-crime risk, Tipico may collect, use and retain personal data for customer and business-partner due diligence, risk assessment, ongoing monitoring, investigations and regulatory reporting. This may include information contained in AML, compliance and due-diligence questionnaires; information relating to beneficial ownership, source of funds, source of wealth and financial background; police conduct certificates, criminal-background information or similar documentation where processing is authorised by applicable law; and information used to assess the financial-crime risk associated with suppliers, vendors, consultants, business partners, beneficial owners and other relevant counterparties.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	9

Tipico may also conduct sanctions, politically exposed person, adverse-media and internal financial-crime screening, assign or record risk classifications, periodically review business relationships, and process information necessary to identify, investigate, escalate and document suspicious activities or other potential financial-crime concerns. Where required or permitted by law, relevant information may be disclosed to Financial Intelligence Units, regulators, law-enforcement agencies and other competent authorities. AML and financial-crime compliance records are retained for the period required by applicable legal and regulatory obligations and, where appropriate, for the establishment, exercise or defence of legal claims.

Where relevant to the services provided, Tipico may collect and review information concerning subcontractors engaged by business partners to assess legal, security, compliance or operational risks.

Due-diligence information may influence whether Tipico enters into, continues, changes or terminates a business relationship. Unless expressly stated otherwise in a particular process, such decisions are not based solely on automated processing producing legal or similarly significant effects for an individual.

7. VISITORS, CONTRACTORS AND PHYSICAL SECURITY

When you visit Tipico premises, Tipico may process personal data to:

- arrange and register your visit;
- verify your identity where proportionate and necessary;
- notify or identify your Tipico host;
- issue and recover visitor badges, access credentials or keys;
- manage access to premises, rooms and restricted areas;
- record incoming deliveries and the collection of mail or parcels;
- record security patrols, guard handovers, relevant occurrences and security observations;
- prevent, detect, investigate and respond to security or safety incidents;
- protect employees, visitors, premises, information and company assets;
- support emergency-response and evacuation procedures; and
- comply with applicable security, health-and-safety and legal requirements.

Depending on the nature of your visit, Tipico may process your name, organisation, host, purpose of visit, arrival and departure times, signature, badge or access details, delivery or parcel collection details, key issuance and return details, contact details where necessary, vehicle details and relevant information recorded in security or incident logs.

Providing the basic personal data required for visitor registration and access control is normally necessary to access Tipico premises. If you do not provide this information, Tipico may be unable to grant or continue access.

Contracted reception or security-service providers may process this information for Tipico, subject to appropriate contractual, confidentiality, security and data-protection obligations. Where a service provider processes personal data for its own independently determined purposes, it is responsible for providing information concerning that processing.

CCTV may be in operation at Tipico premises. Appropriate signage is displayed, and additional information is provided in the applicable CCTV Privacy Policy.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	10

8. WITH WHOM DO WE SHARE PERSONAL DATA?

Tipico limits access to personal data to persons who require it for an authorised purpose. Depending on the relevant processing activity, personal data may be disclosed to:

- authorised employees and functions within the relevant Tipico controller;
- other Tipico Group companies where necessary for procurement, finance, legal, compliance, security, audit, administration or relationship management;
- payment, banking, accounting and audit service providers;
- IT, hosting, communication, support and information-security providers;
- procurement, contract-management and supplier-management providers and systems providers;
- due-diligence, sanctions-screening, fraud-prevention, anti-money laundering, credit-reference and business-information providers;
- professional advisers, including lawyers, auditors, insurers and consultants;
- reception, facilities-management, building-management and security-service providers;
- law-enforcement agencies, courts, regulators, tax authorities and other public bodies where disclosure is required or permitted by law;
- parties involved in an actual or proposed corporate transaction, subject to appropriate confidentiality safeguards; and
- other recipients where you have instructed or authorised Tipico to disclose the information.

Where a recipient processes personal data on Tipico's behalf, Tipico puts appropriate contractual data-protection obligations in place. Where the recipient acts as an independent controller, it is independently responsible for its processing under applicable data-protection law.

Tipico does not sell personal data.

9. INTERNATIONAL TRANSFERS

Some recipients of personal data may be located, or may process personal data, outside the European Economic Area ("EEA").

Where personal data is transferred outside the EEA, Tipico ensures that the transfer is made in accordance with Chapter V GDPR. Depending on the destination and recipient, Tipico may rely on:

- a European Commission adequacy decision;
- the European Commission's Standard Contractual Clauses;
- Binding Corporate Rules;
- another legally recognised transfer mechanism; or
- a derogation under Article 49 GDPR where its conditions are met and its use is appropriate.

Where required, Tipico carries out an assessment of the circumstances of the transfer and applies supplementary contractual, technical or organisational measures.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	11

You may contact the Group Data Protection Officer for information about the applicable transfer mechanism and how to obtain a copy of or information about the relevant safeguards. Certain information may be redacted where necessary to protect confidential or commercially sensitive information.

10. HOW LONG DO WE RETAIN PERSONAL DATA?

Tipico retains personal data only for as long as necessary for the purposes described in this Privacy Statement and to meet applicable legal, regulatory, contractual, accounting, audit and claims-management requirements. The applicable retention period depends on:

- the nature and duration of the business relationship;
- the type of record and the purpose for which it was created;
- statutory accounting, tax, regulatory or compliance obligations;
- applicable limitation periods;
- the need to establish, exercise or defend legal claims;
- ongoing complaints, disputes, investigations, audits or proceedings; and
- Tipico's applicable retention schedule.

The following general periods or criteria apply:

Record category	Retention period or criterion
Unsuccessful supplier proposals and preliminary negotiations	Retained for the period necessary to conclude the selection process and address related queries or claims, in accordance with the applicable retention schedule
Contracts, purchase orders and core relationship records	Duration of the relationship and thereafter for the applicable statutory limitation, accounting, audit or regulatory period
Invoices, payments and accounting records	Retained for the period required by applicable accounting and tax law
Supplier, business-partner, AML and financial-crime due-diligence and screening records	Duration of the relationship and thereafter for the period required by applicable law, regulatory requirements and Tipico's risk and claims-management needs
Business correspondence	Retained according to its subject matter, business relevance and any related contractual, legal or claims period
User accounts and access permissions	Until access is no longer required, followed by deletion or retention of necessary audit evidence in accordance with the applicable security-retention period
Ordinary visitor registration records	Normally 180 days, unless a different location-specific requirement applies
Post and parcel collection records	Normally three years where used to evidence receipt or collection
Key issue and return records	Normally 24 months
Guard handover and foot-patrol records	Normally 12 months
Security occurrence and incident records	Normally up to three years, or longer where linked to an incident, investigation or claim
CCTV footage	Retained for the period stated in the applicable CCTV Privacy Policy or location-specific CCTV notice

Where a record is relevant to an actual or reasonably anticipated investigation, complaint,

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	12

insurance matter, legal claim, regulatory enquiry or law-enforcement request, Tipico may place that record under legal or investigation hold. Normal deletion will be suspended until the relevant matter has been resolved and any applicable retention requirement has expired.

At the end of the applicable retention period, personal data is deleted, destroyed or irreversibly anonymised in accordance with Tipico's retention and deletion procedures.

11. IS PROVIDING PERSONAL DATA MANDATORY?

Certain personal data is necessary for Tipico to:

- assess or enter into a contract;
- administer and perform a business relationship;
- process invoices and payments;
- carry out legally required identity, ownership or compliance checks;
- create necessary system or premises access;
- register visitors and maintain secure premises; or
- comply with legal or regulatory obligations.

Where providing personal data is legally or contractually required, or necessary to enter into or perform a contract, Tipico will indicate this where appropriate.

If required personal data is not provided, Tipico may be unable to:

- evaluate or onboard a supplier or business partner;
- enter into or perform a contract;
- process a payment;
- grant system or premises access;
- complete due-diligence or compliance checks; or
- continue the relevant business relationship.

Personal data requested on a voluntary basis will be identified as such where this is not otherwise apparent from the circumstances.

12. AUTOMATED DECISION-MAKING AND PROFILING

Tipico does not generally make decisions concerning suppliers, business partners or visitors that are based solely on automated processing and that produce legal effects or similarly significantly affect an individual.

Tipico may use automated tools to support screening, fraud prevention, anti-money laundering checks, security monitoring, ESG compliance evidence review, risk assessment or the prioritisation of due-diligence alerts. Unless expressly stated otherwise in a particular process, relevant decisions are subject to proportionate human review and are not made solely by automated means.

If Tipico introduces processing falling within Article 22 GDPR, affected individuals will receive additional information about:

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	13

- the existence of the automated decision-making;
- meaningful information about the logic involved;
- the significance and envisaged consequences of the processing; and
- the applicable rights and safeguards, including the right to obtain human intervention where required by law.

Visitor information is not used for profiling or solely automated decision-making producing legal or similarly significant effects.

13. DATA SECURITY

Tipico is certified according to the DIN ISO/IEC 27001:2022 standard. Tipico applies appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Depending on the relevant processing activity, these measures may include:

- access restrictions based on authorised business need;
- identity and access-management controls;
- confidentiality obligations;
- physical-security controls;
- encryption and other technical safeguards;
- logging, monitoring and audit controls;
- supplier and processor security requirements;
- incident-management procedures;
- staff awareness and training; and
- secure deletion and disposal procedures.

Personal data should be submitted through the communication channel specified by Tipico. Highly confidential personal data should not be sent through unsecured communication channels.

14. YOUR DATA-PROTECTION RIGHTS

Subject to the conditions and limitations set out in applicable data-protection law, you may have the right to:

- request access to your personal data and obtain a copy;
- request correction of inaccurate or incomplete personal data;
- request deletion of personal data;
- request restriction of processing;
- object to processing based on legitimate interests;
- receive personal data you provided in a structured, commonly used and machine-readable format, and request its transmission to another controller, where the right to data portability applies;
- withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing before withdrawal;
- obtain information about applicable international-transfer safeguards; and
- lodge a complaint with a competent supervisory authority.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	14

Right to object

Where Tipico processes personal data on the basis of legitimate interests, you have the right to object on grounds relating to your particular situation. Tipico will stop the relevant processing unless it demonstrates compelling legitimate grounds that override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defence of legal claims. Where personal data is processed for direct-marketing purposes, you may object at any time. Tipico will stop processing the personal data for that purpose.

Rights are not absolute. Tipico may decline or limit a request where permitted or required by law. Tipico may request information necessary to verify your identity before responding.

15. COMPLAINTS AND SUPERVISORY AUTHORITIES

If you have concerns about Tipico's processing of your personal data, you may contact the Group Data Protection Officer so that Tipico has an opportunity to investigate and respond.

You also have the right to lodge a complaint with the data-protection supervisory authority in the country of your habitual residence, place of work or place of the alleged infringement.

Where the relevant controller is established in Malta, the supervisory authority is:

Office of the Information and Data Protection Commissioner
Floor 2, Airways House
Triq Il-Kbira
Tas-Sliema SLM 1549
Malta
Website: [Information and Data Protection Commissioner](#)

16. CONTACTING THE DATA PROTECTION OFFICER

For questions about this Privacy Statement, the processing of your personal data or the exercise of your data-protection rights, please contact:

Group Data Protection Officer
Tipico Group
Tipico Tower
Vjal Portomaso
St. Julian's STJ 4011
Malta
Email: dpo@tipico.com

Please specify the Tipico company, business relationship, premises or processing activity concerned, where known. This will help Tipico identify the relevant controller and respond efficiently.

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	15

17. CHANGES TO THIS PRIVACY STATEMENT

Tipico may update this Privacy Statement to reflect changes in its processing activities, organisational structure, legal obligations or applicable guidance.

The current version will be published on the Tipico Group website. Where a change materially affects the way Tipico processes personal data, Tipico will take appropriate steps to draw attention to that change.

The version number and publication date appear on this Privacy Statement.

18. DOCUMENT CONTROL

Title: PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS

Target audience: Visitors, suppliers, contractors, consultants, couriers and other business partners, including their representatives, personnel, shareholders and beneficial owners.

Classification: PUBLIC

Version: 2.0

Modification: Complete revision to provide more detailed GDPR transparency information and extend the scope to visitors, contractors, couriers and physical-security processing.

Responsible: Group DPO Office

Reviewers: Group Legal, Procurement/Supplier Management, Compliance, Information Security, Office Management and Group DPO Office

Status:	FINAL	Version:	2.0
Classification:	PUBLIC	Date:	11.10.2026
File:	PRIVACY STATEMENT FOR VISITORS AND BUSINESS PARTNERS	Page:	16